A secure process in requesting computer 100 validates the "warranty authorization" and stores validated warranty information (configuration and time periods) in a secure fashion. The secure process may be implemented under security provided by the operating system or it is implemented as a secure processor 150 as described earlier. The "warranty authorization" sent from warranty server 300 to requesting computer system 100 is hashed by warranty server 300 using an algorithm such as Secure Hash Algorithm 1 (SHA-1) and that hash is then encrypted with the warranty server's private key using public key encryption methodology such as the RSA encryption method — producing a warranty authorization that is digitally signed by the warranty server. Warranty server 300 creates a digital certificate for the warranty authorization that includes the encrypted hash , the hash algorithm, and the encryption algorithm.

Secure processor 150 receives the digitally signed "warranty authorization". First, secure processor 150 hashes the "warranty authorization" using the hash algorithm specified by warranty server 300 and decrypts the encrypted hash present in the digital certificate sent by warranty server 300 using the public key – private key encryption method specified in the digital certificate. Secure processor 150 then compares the calculated hash to the decrypted hash to authenticate the warranty authorization. If the two hash values match, the warranty authorization is authentic, i.e. the warranty authorization is known to have come from warranty server 300 and no information within the authorization was changed during the transmission. If the hash values do not match, the authorization is rejected by secure processor 150 as per block 455. Otherwise, the warranty information (configuration, type and time period) is then validated by comparing the warranted configuration to the actual configuration. If the warranted configuration matches the actual configuration, then the warranty authorization is deemed valid and is securely stored by secure processor 150 in secure storage 215. Secure processor 150 is designed to be inaccessible to the user of the computer. The computer user should not be able to alter the warranty information although it is permissible for the user to view the warranty information. One type of limited access secure processor which may be employed as secure processor 150 is a Trusted Computing Platform Alliance (TCPA) secure processor.

As seen in the flow chart of FIG. 5A, another feature of the disclosed methodology involves the automatic recognition of a configuration change by computer system 100 and the provision of an option for the computer user to upgrade the warranty when a configuration change is detected. FIG. 5A details steps in the warranty upgrade program installed in computer system 100 that implement this technology. The warranty upgrade program can run in the background while other programs are executing in computer system 100 as per block 500. The program causes computer 100 to monitor for any changes in its configuration as per decision block 505. If no configuration change is found the computer continues monitoring for configuration changes. However, if a configuration change is found, for example if the user upgrades the hard drive from a 20G drive to a 100G drive, this is detected at decision block 505 and a dialog box appears on the display which asks the computer operator/user if a warranty upgrade is desired to cover the new configuration, as per block 510. Decision block 515 tests to determine if the user desires such an upgraded warranty. If the user does not want to upgrade the warranty, then a delay is imposed in block 520. At some time in the future, the user is again asked if a warranty upgrade is desired. The program provides that this feature can be optionally turned off so as to not annoy the user. The user can also set the value of the time delay provided by delay step 520. However, if decision block 515 determines that the user wants to upgrade the warranty, then a warranty upgrade request is sent to the warranty server 300 as per block 525. The content of this warranty request is substantially the same as the warranty request of step 415 described with respect to the program flow chart of FIG. 3. For example, this warranty request includes computer configuration information and an identification number unique to the particular computer system 100. After the warranty request is sent to the warranty server, warranty processing continues with steps 420 – 455 substantially similar to such processing in the block diagram of FIG. 3.

As seen in the flow chart of FIG. 5B, yet another feature of the disclosed methodology involves the automatic initiation of a warranty request after the first time that computer 100 is operated, i.e. when the warranty is not yet registered with

the warranty server. The user is given the opportunity to opt out and not register the warranty if so desired. When computer 100 is first operated, computer operation starts at block 535 after which the operating system is installed at block 540. Application software is then installed as per block 541. The warranty program is installed at block 542 and run at block 543. The warranty program on computer 100 monitors to determine if the warranty registration has already occurred as per block 545. If it is found that the warranty has already been registered with the warranty server, then process flow returns to other machine operations as per block 550. One way for computer 100 to determine if the warranty has already been registered is to look at the contents of secure storage 215 to see if a warranty authorization is stored therein. If this is the first time that computer 100 has been operated by a user, then the lack of a warranty authorization will be detected. In this event, process flow continues to decision block 555 at which the computer outputs a user query asking the user if she wants to register the warranty with the warranty provider. If the user indicates that she does not want to register the warranty with the warranty provider, then process flow returns to other machine operations as per block 560. However, if it is found that the user wants to register the warranty, then process flow continues to block 410 at which computer configuration data is collected. From block 410 to block 452, process flow is similar to the process flow described with respect to FIG. 3, except that warranty quote step 425 and warranty quote payment step 430 are omitted. Ultimately the warranty authorization is stored in secure processor 215 and warranty registration is complete.

The above has described the operation of computer 100 after operating system installation relative to initial warranty registration. For future sessions after operating system installation, computer operation commences at block 543 such that the user is queried about warranty registration during each computer session until warranty registration occurs. To avoid user annoyance, the warranty program gives the user the opportunity to turn off the warranty registration user query if that is desired. It is noted that the warranty authorization in the secure processor could be factory installed, integrator installed, reseller installed or user installed.